Email Threat Review
Mai 2022

HORNETSECURITY

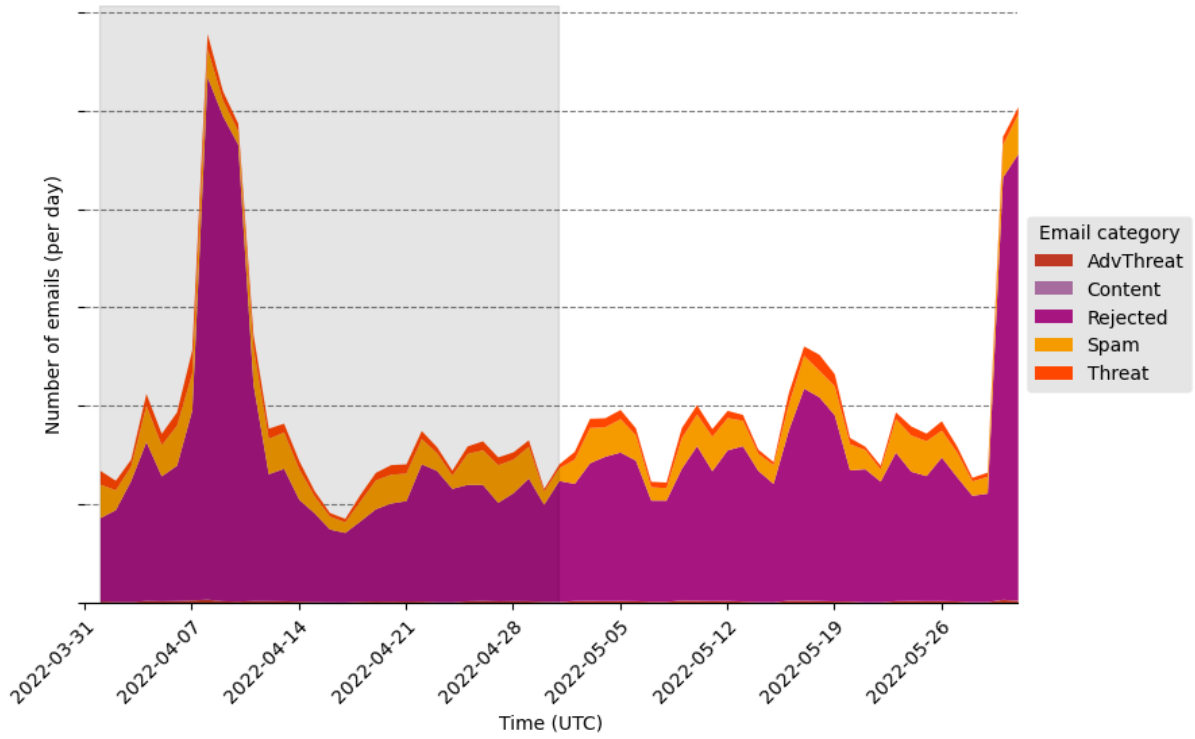
Inhalt

Unerwünschte E-Mails nach Kategorie

Die folgende Tabelle zeigt die Verteilung der unerwünschten E-Mails nach Kategorien.

Email category	%
Rejected	81.81
Spam	13.45
Threat	3.85
AdvThreat	0.85
Content	0.04

Das folgende Zeithistogramm zeigt das E-Mail-Volumen pro Kategorie und Stunde.



Methodik

Die aufgelisteten E-Mail-Kategorien entsprechen den E-Mail-Kategorien, die im Email Live Tracking des Hornetsecurity Control Panels aufgelistet sind. Unsere Benutzer sind also bereits mit ihnen vertraut. Für andere sind die Kategorien:

Kategorie	Beschreibung
Spam	Diese E-Mails sind unerwünscht und haben häufig einen werblichen oder betrügerischen Charakter. Die E-Mails werden gleichzeitig an eine große Anzahl von Empfängern verschickt.
Content	Diese E-Mails haben einen ungültigen Anhang. Welche Anhänge ungültig sind, legen die Administratoren im Modul Content Control fest.
Threat	Diese E-Mails enthalten gefährliche Inhalte wie bösartige Anhänge oder Links oder werden zur Begehung von Straftaten wie Phishing verschickt.
AdvThreat	Bei diesen E-Mails hat Advanced Threat Protection eine Bedrohung erkannt. Die E-Mails werden für illegale Zwecke eingesetzt und nutzen

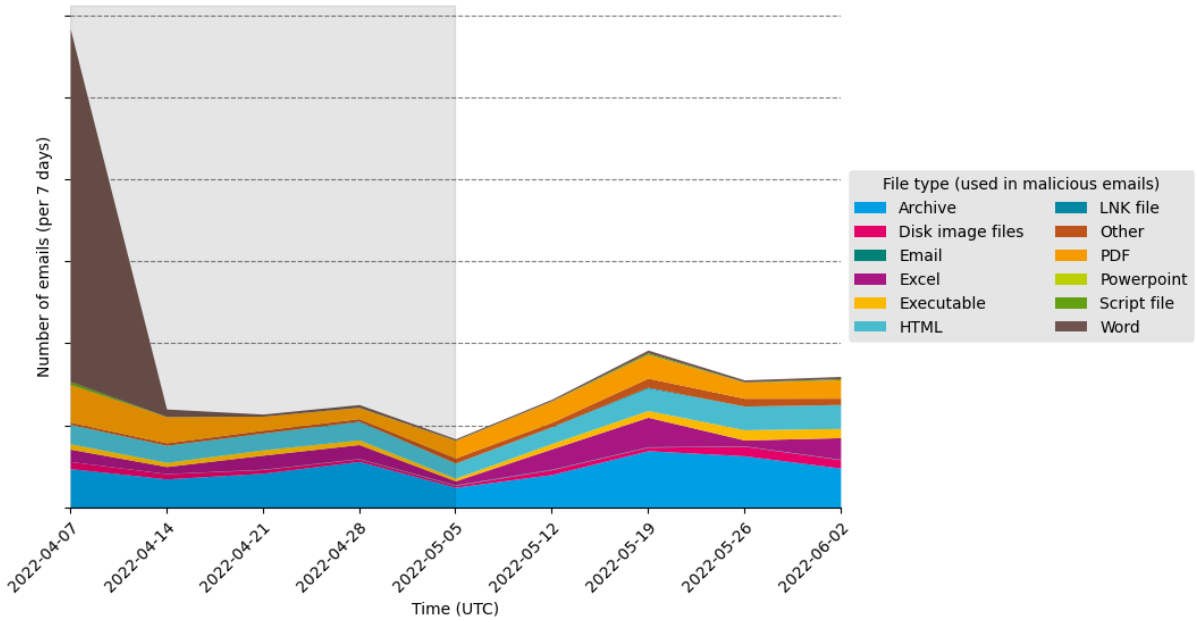
Kategorie	Beschreibung
	ausgeklügelte technische Mittel, die nur mithilfe von fortgeschrittenen dynamischen Verfahren abgewehrt werden können.
Abgelehnt	Diese E-Mails werden aufgrund externer Merkmale, die z. B. die Identität des Absenders betreffen können, im Laufe des SMTP-Dialogs direkt von unserem E-Mail-Server abgelehnt und nicht weiter analysiert.

Bei Angriffen verwendete Dateitypen

Die folgende Tabelle zeigt die Verteilung der in Angriffen verwendeten Dateitypen.

Dateityp (verwendet in bösartigen E-Mails)	%
Archive	33.8
HTML	17.0
PDF	16.4
Excel	13.7
Executable	5.8
Other	5.6
Disk image files	4.7
Word	1.7
Script file	0.6
Email	0.4
LNK file	0.3

Das folgende Histogramm zeigt das E-Mail-Volumen pro Dateityp, das bei Angriffen innerhalb von sieben Tagen verwendet wird.

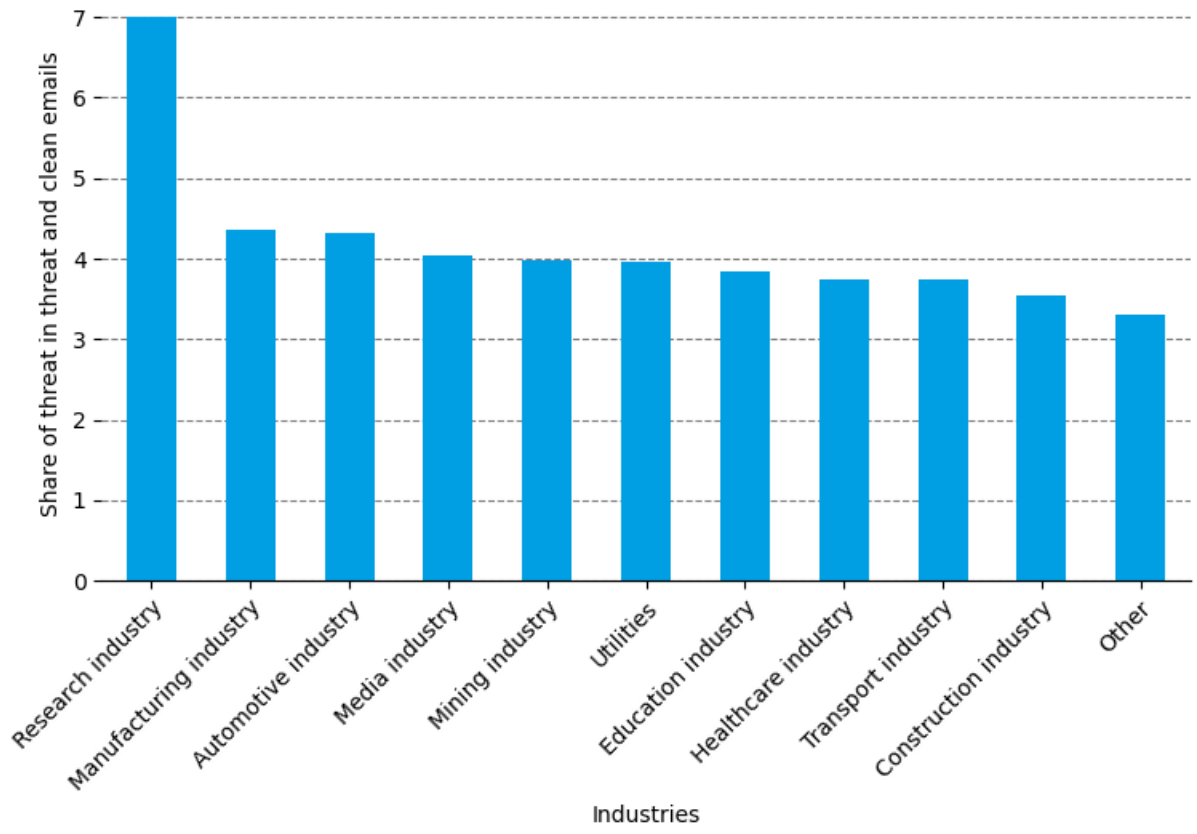


Branchen Email Threat Index

Die folgende Tabelle zeigt unseren Branchen-E-Mail-Bedrohungsindex, der auf der Anzahl der schadhaften E-Mails im Vergleich zu den gültigen E-Mails der einzelnen Branchen (im Median) basiert.

Branchen	Anteil der Threat Emails an Threat und Gültigen Emails
Research industry	7.0
Manufacturing industry	4.4
Automotive industry	4.3
Media industry	4.0
Mining industry	4.0
Utilities	4.0
Education industry	3.8
Healthcare industry	3.7
Transport industry	3.7
Construction industry	3.6

Das folgende Balkendiagramm visualisiert die E-Mail-basierte Bedrohung für jede Branche.



In diesem Monat ist der Bedrohungsindex für die Forschungsindustrie gestiegen. Andere Branchen weisen einen leicht entspannten Bedrohungsindex im Vergleich zum Vormonat auf.

Methodik

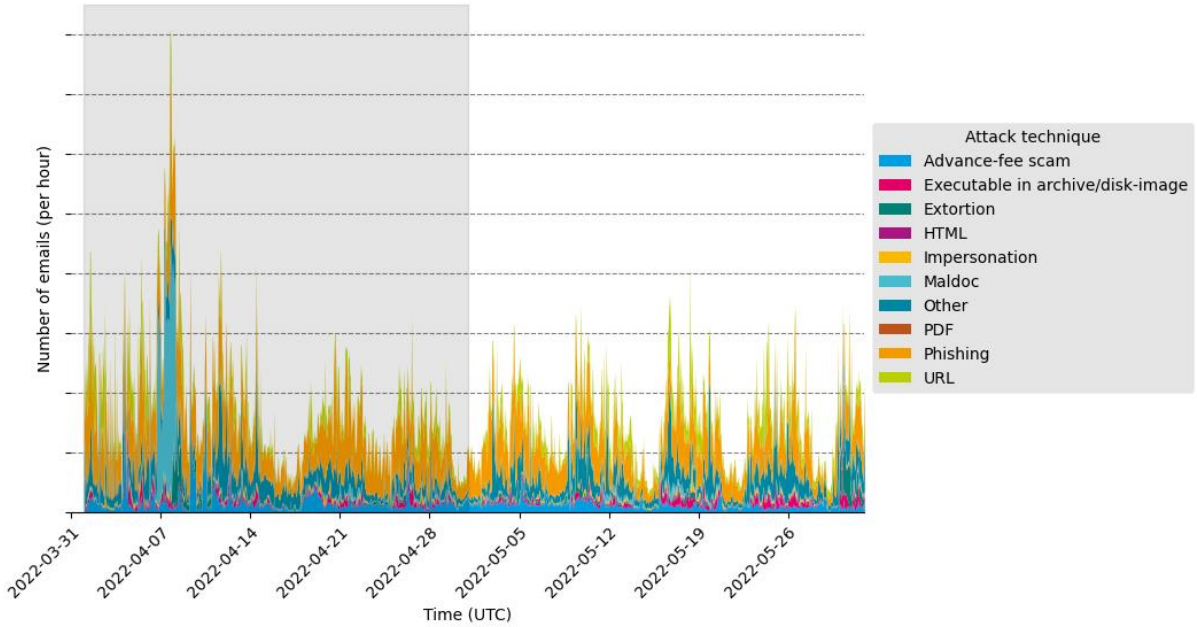
Unterschiedlich große Organisationen erhalten eine unterschiedliche absolute Anzahl von E-Mails. Um Organisationen zu vergleichen, haben wir daher den prozentualen Anteil der Threat E-Mails an den Threat und Gültigen E-Mails jeder Organisation berechnet. Anschließend berechnen wir den Median dieser Prozentwerte über alle Organisationen innerhalb derselben Branche, um den endgültigen Threat Index für die Branche zu ermitteln.

Angriffstechniken

Die folgende Tabelle zeigt die bei Angriffen verwendete Angriffstechnik.

Angriffstechnik	%
Phishing	40.0
URL	14.9
Advance-fee scam (dt. Vorschussbetrug)	7.8
Executable in archive/disk-image	4.3
Extortion	4.0
Impersonation	2.0
Maldoc	1.4
HTML	1.3
PDF	0.3
Other	23.9

Das folgende Zeithistogramm zeigt das E-Mail-Volumen pro eingesetzter Angriffstechnik pro Stunde.



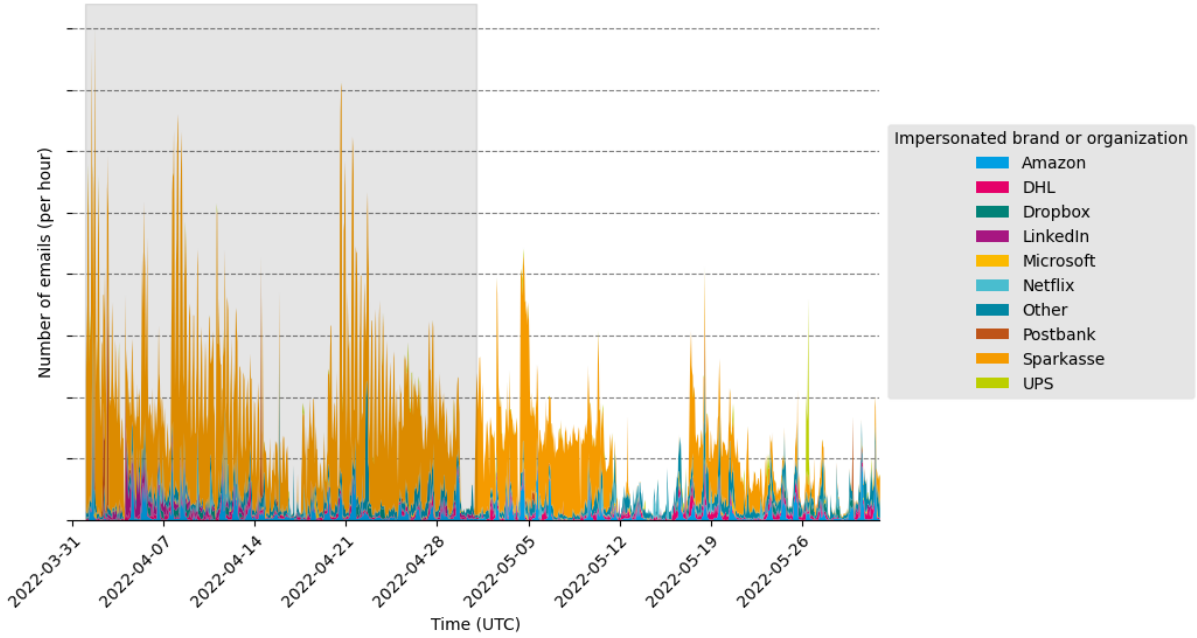
Attack techniques

Imitierte Firmenmarken oder Organisationen

Die folgende Tabelle zeigt, welche Firmenmarken unsere Systeme am häufigsten bei Impersonationsangriffen entdeckt haben.

Imitierte Firmenmarke oder Organisation	%
Sparkasse	60.9
Amazon	7.6
DHL	5.6
UPS	2.1
Dropbox	1.6
Microsoft	1.5
Netflix	1.4
LinkedIn	1.4
Fedex	1.2
Volks- und Raiffeisenbank	1.1
1&1	1.0
Postbank	1.0
Other	13.6

Das folgende Zeithistogramm zeigt das E-Mail-Volumen für Firmenmarken, die bei Impersonationsangriffen entdeckt wurden, pro Stunde.



Obwohl wir einige Pausen in den laufenden Sparkassen-Phishing-Kampagnen beobachtet haben, dominiert die Sparkasse weiterhin unsere Charts.

Hornetsecurity GmbH · Am Listholze 78 · 30177 Hannover GERMANY
Tel.: +49 511 515 464-0 · info@hornetsecurity.com · www.hornetsecurity.com
VAT ID: DE256599255 · CEOs: Daniel Hofmann, Daniel Blank · County court Hannover · HRB 201937
Hannoversche Volksbank · IBAN: DE74 2519 0001 0573 5742 00 · BIC: VOHADE2H